Modeling and Simulation 建模与仿真, 2025, 14(7), 140-153
Published Online July 2025 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2025.147523

Hans汉斯

隐私保护下基于XGBoost-LightGBM融合模型用电数据异常检测

孙　慧，智路平

上海理工大学管理学院，上海

收稿日期：2025年6月21日；录用日期：2025年7月14日；发布日期：2025年7月23日

摘　要

据Northeast Group报导，全球由于窃电造成的经济损失高达960亿美元/年，对发达国家和发展中国家用电安全均产生了严重影响，为了减少窃电损失，亟需提升用户侧用电数据异常检测的安全性和效率。本研究在传统的电力数据异常检测框架上引入基于AES + RSA的混合加密架构，并结合SHA-256加密哈希算法和数字签名技术实现数据传输的安全性保护、完整性验证与身份认证；在异常检测阶段，利用网格搜索对XGBoost与LightGBM模型进行参数优化后，通过构建以AUC与预测差异性为动态权重调整因子的模型融合式，使优化后的XGBoost与LightGBM模型实现自适应融合以提升检测方法的泛化性。利用国家电网公开数据集进行检测实验，结果显示该模型AUC达到了82.03%，Accuracy为91.53%，G-mean值为54.99%，继而在4个KEEL公开数据集上进行泛化性能测试，结果表明该检测方法具有较好的检测异常样本的能力。

关键词

异常检测，混合加密，XGBoost，LightGBM，差异性

Privacy-Preserving Electricity Consumption Anomaly Detection Based on XGBoost-LightGBM Hybrid Model

Hui Sun, Luping Zhi

Business School, University of Shanghai for Science and Technology, Shanghai

Received: Jun. 21st, 2025; accepted: Jul. 14th, 2025; published: Jul. 23rd, 2025

Abstract

According to a Northeast Group report, electricity theft causes up to USD 96 billion in annual global

文章引用: 孙慧, 智路平. 隐私保护下基于 XGBoost-LightGBM 融合模型用电数据异常检测[J]. 建模与仿真, 2025, 14(7): 140-153. DOI: 10.12677/mos.2025.147523

economic losses, severely compromising power security in both developed and developing nations. To mitigate these losses, enhancing the security and efficiency of user-side power-consumption anomaly detection is imperative. This study extends the conventional anomaly-detection framework by integrating a hybrid encryption scheme based on AES and RSA, combined with SHA-256 hashing and digital-signature techniques, to ensure data confidentiality, integrity verification, and authentication during transmission. In the anomaly-detection phase, the research first employs grid search to optimize hyperparameters for XGBoost and LightGBM models. The authors then fuse the optimized models via a dynamic weighting mechanism where weights are adaptively adjusted based on each model's AUC and prediction diversity, thereby improving the ensemble's generalization capability. Experimental evaluation on a publicly available State Grid dataset demonstrates that the proposed hybrid model achieves an AUC of 82.03%, an accuracy of 91.53%, and a G-mean of 54.99%. Generalization tests on four KEEL benchmark datasets confirm the method's robust anomaly detection capability.

Keywords

Anomaly Detection, Hybrid Encryption, XGBoost, LightGBM, Diversity

1. 引言

电力盗窃在发达国家和发展中国家都是一个日益严重的问题。发展中国家每年约有 50%的电力盗窃情况。窃电在发达国家也造成了巨大的经济损失，对于美国和英国来说，每年能源盗窃造成的经济损失从 1 到 60 亿不等[1]。因此，检测电力盗窃是一项切实的产业需求，催生了多种实用技术，但实践表明，现有检测方法的通用性与可靠性有待进一步提升。同时，由于检测导致的电力数据传输隐私泄露也产生了明显的舆情问题，如美国电信巨头 Verizon 公司发布的《数据泄露调查报告(DBIR)》显示，采矿与公用(电力)事业合并行业历年均发生数起数据泄露事件，其中确认数据泄露的事件占约 60%，由其产生的网络舆情影响广泛，这是其他网络舆情所无法比拟的[2]。因此，检测异常用电还需考虑数据隐私保护问题。

目前异常用电检测的方法大致分为三类：知识驱动、物理驱动和数据驱动。知识驱动通常依赖于先验的领域知识和理论模型进行主观分析，主观性较强[3]。物理驱动通常依赖于冗余设备部署来监测用户的用电量，然而设备折损率、运维复杂度和维护成本均较高。数据驱动是目前的主流检测方法，此方法以大数据分析为基础，以机器学习或深度学习为技术手段，进行准确且快速地检测。

早期的窃电检测主要依赖稀疏表示方法，周李等[4]提出一种使用稀疏编码的模型，结合字典学习的方法，通过各个特征的使用频率来判断异常值。许刚[5]提出一种基于稀疏随机森林模型的用电侧异常行为模式检测方法。夏晓芳等[6]提出自适应二进制拆分检查(ABSI)算法，通过分组测试大幅降低了排查成本，但因其对特征关联性挖掘不足，难以捕捉深层次的异常信号。随着深度学习兴起，郑子斌等[7]提出了一种基于卷积神经网络(CNN)模型的窃电检测方法来进行电量的异常检测，当训练集占总数据集的60%时，达到最佳 AUC79.22%。Nabil 等[8]提出一种基于广义深度递归神经网络(RNN)的电力盗窃探测器。张宇帆等[9]提出利用深度卷积生成对抗网络鉴别器提取得到的特征，在边缘数据中心对二范数线性支持向量机进行窃电检测。Javaid 等[10]提出了卷积神经网络(CNN)和长短期记忆(LSTM)相结合的深度连体网络来区分诚实电力消费者和欺诈电力消费者的特征。高欣等[11]提出一种基于条件变分自编码器－

卷积神经网络(CVAE-CNN)模型的分类方法，提高对少数类别的识别率。严莉等[12]提出一种基于图注意力和 Transformer 的异常检测模型进行异常检测。蔡梓文等[13]提出构建多维度特征提取变分自编码器(MF-VAE)来提取用户用电行为的多维度特征。针对单一模型的泛化能力不足问题，游文霞等[14]提出一种基于 Bagging 异质集成学习的窃电检测方法，构建多种个体学习器嵌入的 Bagging 异质集成学习的窃电检测模型。李国成等[15]提出一种基于 Bagging 二次加权集成的孤立森林窃电检测算法，对各类窃电模式的孤立特征顺序进行优选并训练对应的孤立森林模型。基于上述分析，稀疏表示方法在面对多样化窃电模式时表现受限，深度学习虽然在复杂特征提取上具备优势，却存在训练成本高、可解释性差及泛化能力不足等问题。

在窃电检测领域中，数据传输送至检测的过程中的隐私性也是应当考虑的问题。Naim 等[16]提出一种基于 RSA 加密算法的窃电检测方法，该方法使用 RSA 算法对电量测量值进行加密，防止未加密的用电数据在传输过程中被第三方窃取或监视，但该方法效率较慢，会造成资源浪费。目前仅有个别文献考虑了传输过程中的隐私泄漏问题，没有很好地解决大数据隐私保护这一热点问题，且数据传输真实性和完整性等问题亟需解决。

针对以上存在的问题，本文基于国家电网公开数据集，在进行数据传输隐私保护的前提下，使用 XGBoost 与 LightGBM 融合模型进行用电数据异常检测。本文工作集中在以下两个方面：a) 引入 AES + RSA 混合加密算法结合 SHA-256 和数字签名，确保数据在传输过程中的安全性、完整性与真实性；b) 基于网格搜索对 XGBoost 与 LightGBM 模型进行参数优化后，构建以 AUC 与预测差异性为动态权重调整因子的模型融合式，使优化后的 XGBoost 与 LightGBM 模型实现自适应融合，提升检测方法的泛化性。

2. 模型

本文提出使用 AES + RSA 混合加密算法结合 SHA-256 和数字签名的方法对数据传输进行隐私保护，基于网格搜索对 XGBoost 与 LightGBM 模型进行参数优化后，进行以 AUC 与预测差异性为动态权重调整因子的自适应加权融合，以此构建用电数据异常检测框架。该框架如图 1 所示。

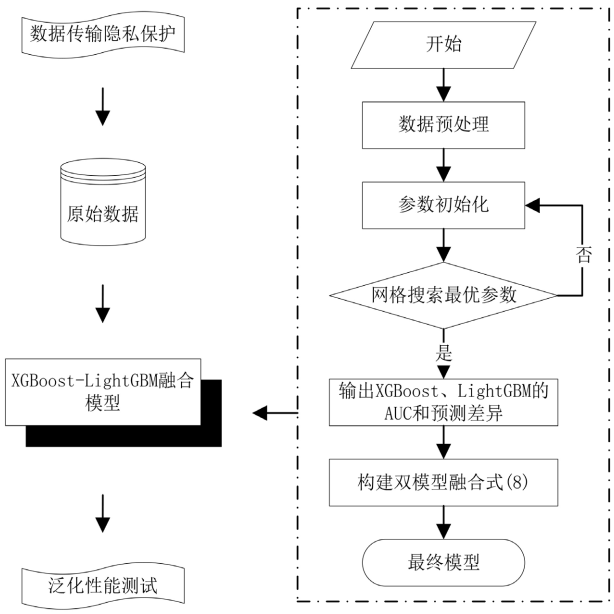


Figure 1. Abnormal electricity consumption detection framework
图 1. 用电数据异常检测框架

2.1. AES + RSA 混合加密结合 SHA-256 和数字签名的数据传输隐私保护模型

针对电力场景中电力数据的安全传输需求，本文创新性地引入了基于 AES＋RSA 混合加密的隐私保护框架，并结合 SHA-256 哈希算法与数字签名技术，有效解决电力系统在智能电表数据采集场景下面临的数据传输安全性、完整性和身份真实性的问题。

2.1.1. AES + RSA 混合加密

加密算法主要分为对称加密和非对称加密。对称加密常见算法包括：DES、3DES 和 AES，非对称加密常见算法包括：RSA、DSA 和 ECC。对称加密由于算法简单，导致在处理大数据量时加密速度比非对称加密快得多，但其在加密和解密过程使用相同的密钥，一旦密钥被泄露，窃取者可轻易地获取通信信息。非对称加密虽然安全性高，只要私钥进行保密，就能保证通信信息的安全，但其计算成本较高，相比于对称加密，非对称加密在处理大数据量时性能较差，速度较慢。

因此，考虑到对称加密的速度优势和非对称加密的安全性，本文选择采用 AES＋RSA 的混合加密系统，既保证了通信的安全性，也不影响通信的效率。该系统过程如图 2 所示。

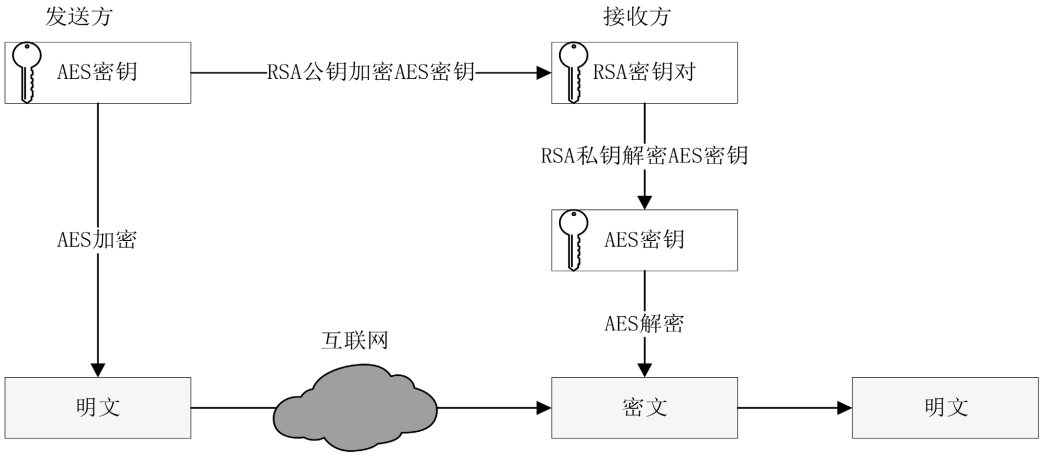


Figure 2. AES + RSA hybrid encryption process
图 2. AES + RSA 混合加密过程

2.1.2. SHA-256

当前的哈希算法主要分为加密哈希算法和非加密哈希算法，其中，加密哈希算法包括 MD5、SHA-1、SHA-2、SHA-3、BLAKE 系列、RIPEMD 系列和 Whirlpool 等；非加密哈希算法包括 CRC 系列、MurmurHash、CityHash 和 SipHash 等。加密哈希算法主要用于数据完整性验证和数字签名等场景，更具安全性，而非加密哈希算法主要用于数据结构和快速查找等场景，侧重于速度和均匀分布性，不保证安全性。

由于本文的应用场景为电力场景，其数据传输涉及敏感信息，更需其与数字签名结合实现身份认证，确保数据来源可靠性。因此，本文选用抗碰撞性强、安全性和成熟度均较高的 SHA-256 加密哈希算法。

SHA-256 加密哈希算法作用机理是对输入数据进行两个阶段的处理：预处理和摘要计算。其作用机理如图 3 所示。预处理将输入消息格式化为规范结构，先输入任何二进制形式的原始消息，对其进行消息填充，再将填充后的消息分割为多个 512bit 块，记为 M(0)，M(1)，...，M(N − 1)，每个块进一步划分为 16 个 32bit 字，记为 W0，W1，...，W15。在摘要计算阶段，先初始化哈希值 H0，H1，...，H7，对每个 512bit 块 M(i)进行消息扩展，将 16 个 32bit 字 W0，W1，...，W15 扩展为 64 个 32bit 字 W0，W1，...，W63，扩展公式为：

$$W_t = \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-16}) \tag{1}$$

再进行初始化 8 个工作变量 A，B，C，D，E，F，G，H，其初始值为当前哈希值 H(i)，执行 64 轮迭代计算，不断更新哈希值，处理完所有消息块后，将最终的 H(N)拼接起来，得到 256 位哈希摘要。

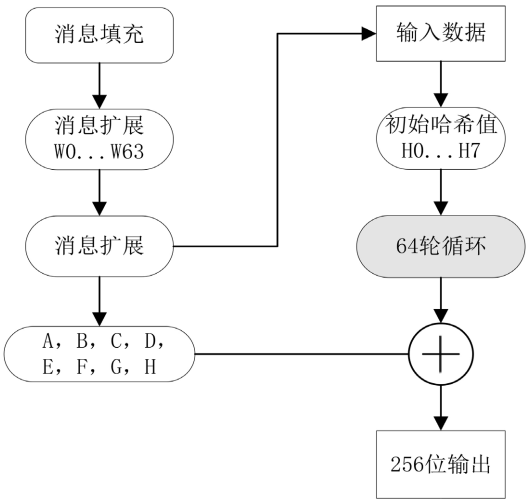


Figure 3. Operational principle of SHA-256
图 3. SHA-256 作用机理

2.1.3. 数字签名

数字签名通过使用加密算法来确定数据的有效性，其签名过程如图 4 所示。具体定义如下：

初始化产生签名的基本参数$(KeyGen, Sign, Verify)$，其中，$KeyGen$ 为密钥生成算法集合，$Sign$ 为签名算法集合，$Verify$ 为验证算法集合。在密钥生成算法中输入安全参数 λ，随机输出一对密钥(sk, pk)，其中 sk (私钥)用于签名，pk (公钥)用于验证签名；在签名算法中输入私钥 sk 和消息 m，随机输出签名 σ；在验证算法中输入公钥 pk、消息 m 和签名 σ，输出一个 $bit\{0,1\}$，其中，输出 1 表示签名有效，输出 0 表示签名无效。

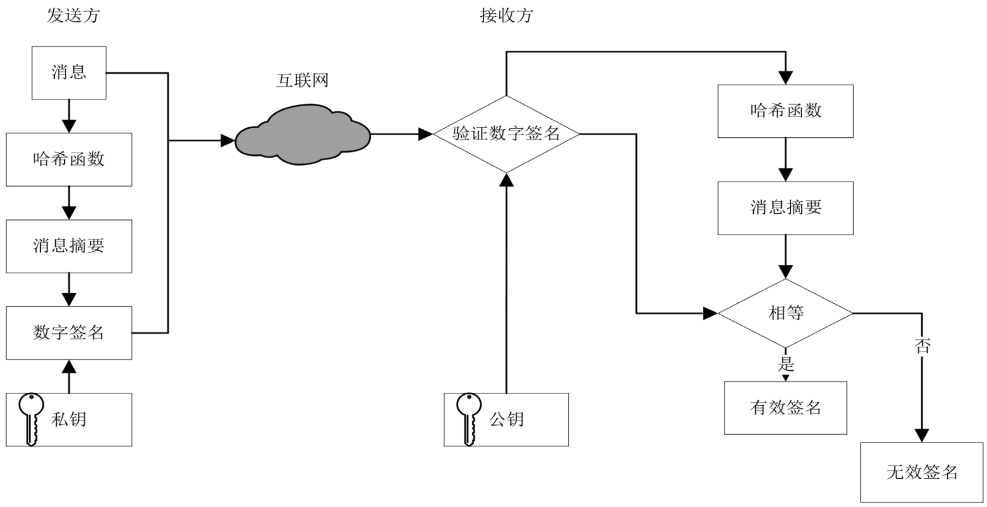


Figure 4. Digital signature process
图 4. 数字签名过程

2.2. 优化的 XGBoost 模型

XGBoost 基于梯度提升机制，通过逐层叠加决策树以最小化可微目标函数，其核心思想在于通过迭代式集成学习策略优化模型的预测性能。其目标函数由损失函数与正则化项复合构成，公式如下：

$$L=\sum_{i=1}^{n} l\left(y_i, y_i^t\right)+\sum_{k=1}^{t} \Omega\left(f_t\right) \tag{2}$$

其中，$l\left(y_i, y_i^t\right)$ 是衡量预测值与真实值偏差的损失函数，$\Omega\left(f_t\right)$ 是正则化项，通过对模型复杂度进行约束，抑制过拟合。

在迭代优化过程中，模型采用二阶泰勒展开逼近损失函数，并通过贪心策略构建决策树结构。具体而言，模型在每个特征划分点选择时，通过最大化结构分数增益确定最优分裂方案，预测值的更新遵循增量式集成策略，公式如下：

$$y_i^{t+1}=y_i^t+\eta f_t\left(x_i\right) \tag{3}$$

其中，y_i^t 是第 t 轮迭代中的预测值，η 是学习率，用于控制每棵树对整体模型的贡献，$f_t\left(x_i\right)$ 是第 t 轮迭代中训练出来的新决策树对样本 x_i 的预测值。

针对类别不平衡问题，本文在 XGBoost 中建立样本权重机制，通过调整正类样本权值 ω 重构损失函数，公式如下：

$$L=\sum_{i=1}^{n} \omega_i \bullet l\left(y_i, y_i^t\right)+\sum_{i=1}^{t} \Omega\left(f_i\right) \tag{4}$$

其中，ω_i 是第 i 个样本的权重，$\sum_{i=1}^{t} \Omega\left(f_i\right)$ 为正则项，控制模型复杂度。

为了进一步提高模型的性能，在超参数优化阶段，采用网格搜索与 k 折交叉验证相结合的方法，重点优化最大树深度(max_depth)、决策树数量(n_estimators)和学习率(learning_rate)等关键参数。通过 AUC-ROC 曲线作为主要评估指标，经过多轮迭代筛选，确定出最优参数组合，保证模型在测试集上的强泛化性与鲁棒性。

2.3. 优化的 LightGBM 模型

LightGBM 基于梯度提升框架，采用高效直方图算法与 Leaf-wise 生长策略，在提升模型训练速度的同时兼顾预测精度。其目标函数同样由损失函数与正则化项共同构成，公式如下：

$$L=\sum_{i=1}^{n} \omega_i \bullet l\left(y_i, y_i^{t-1}\right)+\sum_{k=1}^{K} \Omega\left(f_k\right) \tag{5}$$

其中，$l\left(y_i, y_i^{t-1}\right)$ 表示损失函数，$\Omega\left(f_k\right)$ 表示正则化项，f_k 表示第 k 棵树的复杂度。

引入基于直方图的特征离散化方法优化 LightGBM，将连续特征转化为离散直方图区间，大幅降低分裂点计算复杂度。同时，其采用 Leaf-wise 树生长策略，每次迭代选择增益最大的叶子节点进行分裂，而非传统 Level-wise 的层遍历方式，从而实现更快的收敛速度与更高的模型效率。模型更新预测值公式如下：

$$y_i^t=y_i^{t-1}+\eta f_t\left(x_i\right) \tag{6}$$

其中，y_i^{t-1} 是第 $t-1$ 轮的预测值，$f_t\left(x_i\right)$ 是第 t 轮构建的决策树对样本 x_i 的预测值。

针对类别不平衡问题，本文同样地在 LightGBM 中建立样本权重机制，通过调整正类样本权值 ω 重构损失函数，公式如下：

$$L=\sum_{i=1}^{n} \omega_i \bullet l\left(y_i, y_i^{t-1}\right)+\sum_{k=1}^{K} \Omega\left(f_k\right) \tag{7}$$

在超参数调优阶段，采用与 XGBoost 相同的网格搜索和 k 折交叉验证相结合的策略，重点优化叶子

节点数量(num_leaves)、最大树深度(max_depth)和决策树数量(n_estimators)等关键参数。此外，模型引入早停机制(early_stopping)动态控制训练轮次，避免过拟合并提升训练效率。

2.4. 多模型融合

单一模型往往会有陷入局部最小点的风险[17]。多个学习器的有效结合，在保证整个模型性能的基础上，每个模型之间的预测差异性越大，模型的融合效果越好，鲁棒性也会越强。本文基于单个模型的 AUC 指标和预测差异性构建出 XGBoost 和 LightGBM 的双模型融合式。设验证集样本数为 N，测试集样本数为 M，最终融合预测概率加权为：

$$P^{(j)} = \omega_{xgb} \bullet P_{xgb}^{(j)} + \omega_{\lg b} \bullet P_{lgb}^{(j)}, j = 1,2,\cdots,M \tag{8}$$

融合模型预测差异性式如下：

$$D = \frac{1}{N}\sum_{i=1}^{N}\left|P_{xgb}^{(i)} - P_{\lg b}^{(i)}\right| \tag{9}$$

其中，D 为预测差异性，$P_{xgb}^{(i)}$ 为 XGBoost 对第 i 个验证样本的预测概率，$P_{\lg b}^{(i)}$ 为 LightGBM 对第 i 个验证样本的预测概率，

XGBoost 和 LightGBM 各自的权重系数定义如下式：

$$\omega_{xgb} = \frac{(1-\alpha)\bullet \mathrm{AUC}_{xgb} + \alpha \bullet D}{(1-\alpha)\left(\mathrm{AUC}_{xgb} + \mathrm{AUC}_{\lg b}\right) + 2\alpha \bullet D} \tag{10}$$

$$\omega_{\lg b} = \frac{(1-\alpha)\bullet \mathrm{AUC}_{\lg b} + \alpha \bullet D}{(1-\alpha)\left(\mathrm{AUC}_{xgb} + \mathrm{AUC}_{\lg b}\right) + 2\alpha \bullet D} \tag{11}$$

其中，AUC_{xgb} 为 XGBoost 在验证集上的 AUC 值，$\mathrm{AUC}_{\lg b}$ 为 LightGBM 在验证集上的 AUC 值，α 为平衡系数，调节预测差异性对权重的影响，

当 $\alpha = 0$ 时，权重完全依赖于 AUC 得分；

当 $\alpha = 1$ 时，权重仅取决于差异权重；

当 $0 < \alpha < 1$ 时，既考虑模型整体性能，也考虑单个模型局部预测差异。

3. 实验

3.1. 数据传输隐私保护

本文通过 AES+RSA 混合加密算法结合 SHA-256 和数字签名，构成数据传输隐私保护安全架构。其具体步骤如下：

a) 非对称加密层使用 RSA-2048 算法，选用 65537 并配置 OAEP 填充方案，其中哈希函数与掩码生成函数均采用 SHA-256 实现；其次，针对对称加密层，选定 AES-256 作为核心算法，采用 CFB 模式配合 128 位初始化向量(IV)；最后，规定数据封装格式为严格字段顺序，包括协议版本号(4 字节)||IV (16 字节) ||RSA 加密的 AES 密钥(256 字节) ||AES 密文||明文哈希(32 字节)||签名(256 字节)；

b) 生成 RSA 主密钥对 private_key ← rsa.generate_private_key (public_exponent = 65537, key_size = 2048)，导出公钥 public_key ← private_key.public_key ()并绑定 X.509 证书，将公钥发给发送方，私钥加密存储在 HSM；

c) 调用 os.urandom (32)生成 32 字节真随机数作为 AES-256 密钥，同时生成 16 字节 IV 向量，向明文头部添加时间戳(8B)和随机数(16B)；

d) 对数据明文 plaintext 使用 SHA-256 得到固定长度摘要 data_hash；再使用发送方私钥签名生成数字签名 signature ← Sign_SK(H)；

e) 使用 AES-256 密钥和 IV 对明文执行 CFB 模式加密，生成 ciphertext；再用接收方公钥通过 RSA-OAEP 加密 AES 密钥，生成 encrypted_key;

f) 按格式序列化所有字段(版本号、IV、encrypted_key、ciphertext、data_hash、signature)；再发送完整数据包，并销毁临时生成的 AES 密钥和 IV；

g) 解析接收的数据包，校验字段长度和版本号，若异常则触发警报并终止流程，若正常，则提取 IV、encrypted_key、ciphertext、data_hash 和 signature 字段；

h) 用私钥解密 encrypted_key 获取 AES 密钥，若 OAEP 填充校验失败则立即中止；使用 AES 密钥和 IV 对 ciphertext 执行 CFB 模式解密，还原原始明文，其中包含时间戳和随机数；

i) 对解密后的明文计算 SHA-256 哈希值 H'，与传输的 data_hash 严格比对；再用发送方公钥验证 signature 是否为 data_hash 的有效签名，若任一校验失败则视作无效签名并擦除会话密钥；

j) 检查明文头部的时间戳和随机数，拒绝过期或重复请求；最后从内存中安全清除解密后的明文和会话密钥。

3.2. 数据预处理

本文使用的窃电数据集来源于国家电网(SGCC)公布的真实数据。数据集包含 1035 天(2014 年 1 月 1 日~2016 年 10 月 31 日)内 42372 位用户的用电数据。

本文操作系统为 Windows10 专业版，硬件为 Intel(R) Xeon(R) CPU E5-2670 v3 @ 2.30GHz/2.30 GHz(2 个处理器)，运行内存为 128GB，实验环境为 PyCharm Community Edition 2020.1.3，Python 版本为 3.6.15，scikit-learn 版本为 0.24.2。

由于智能电表可能出现过故障等实际问题，记录下来的电力数据往往会出现缺失或者异常的情况。在本文中，对于缺失值，选择采用线性插值的方法进行处理：

若当前值 x_i 是缺失值，并且前后相邻的值 x_{i-1} 和 x_{i+1} 均不是缺失值，则使用前后相邻值的平均值进行插值，公式如下：

$$f\left(x_i\right)=\frac{x_{i-1}+x_{i+1}}{2} \tag{12}$$

式中，x 表示某用户的每日用电量向量，x_i 表示该用户在第 i 天的用电量。

若当前值 x_i 是缺失值，但前一个值 x_{i-1} 或后一个值 x_{i+1} 也是缺失值，则插入 0，即 $f\left(x_i\right)=0$；

若当前值 x_i 不是缺失值，则保存当前原始值，即 $f\left(x_i\right)=x_i$。

而对于异常值，采用“2σ 法则”进行修正，公式如下：

$$f\left(x_i\right)=\begin{Bmatrix} avg\left(x\right)+2\bullet std\left(x\right), \text{如果} x_i>avg\left(x\right)+2\bullet std\left(x\right) \\ x_i \end{Bmatrix} \tag{13}$$

式中，$avg\left(x\right)$ 是 x 的平均值，$std\left(x\right)$ 是 x 的标准差。

最后，对用电数据进行归一化，公式如下：

$$f\left(x_i\right)=\frac{x_i-\min\left(x\right)}{\max\left(x\right)-\min\left(x\right)} \tag{14}$$

式中，$\min\left(x\right)$ 为 x 中的最小值，$\max\left(x\right)$ 为 x 中的最大值。

3.3. 评估指标

在本文的数据集中，42372 位用户中有 3615 位用户是窃电用户，窃电用户占总用户人数的 8.53%，即正常用户与窃电用户的不平衡率为 11.72。由此可见，正常样本与异常样本的比例严重失衡，许多模型倾向于关注正常样本的检测准确率，而这种倾斜可能导致模型在识别异常情况时出现较高的误检率(False Positive Rate)和漏检率(False Negative Rate)。在这种情况下，模型的整体准确率(Accuracy)可能高达 99%，但没有识别出任何窃电行为。为此，选用 AUC 作为主要参考指标，它可以反映在不同阈值下对正常行为和窃电行为分类的综合能力，Accuracy 和 G-mean 作为补充指标。G-mean (几何均值)能够更加专注于在不平衡数据中平衡模型对正类和负类的分类表现。

此外，对于二分类问题，利用混淆矩阵来进一步判断模型的可靠性。表 1 所示的混淆矩阵可以帮助了解模型在分类正常用户和窃电用户时的表现。这些信息有助于全面评估模型的分类能力和在实际应用中的效果。

Table 1. Confusion matrix
表 1. 混淆矩阵

实际\检测	检测正常用户	检测窃电用户
实际正常用户	TN (真反例)	FP (假正例)
实际窃电用户	FN (假反例)	TP (真正例)

3.4. 实验结果分析

Ravid 和 Amitai [18]基于 11 个数据集的实验表明，在表格数据场景上，XGBoost 在数据集上的性能表现显著优于深度学习模型(如 TabNet、NODE、DNF-Net 和 1D-CNN)。究其原因，表格数据(如本文所用的电力数据)的特征通常缺乏空间或时间局部性，且呈现稀疏性与无序性，这导致依赖局部特征卷积的 CNN 等深度学习模型难以捕捉有效特征，而基于树模型的 XGBoost 与 LightGBM 不仅能有效处理混合类型特征，还规避了 CNN 对复杂特征工程的依赖，提高了模型效率和性能。

因此，为探究本文模型的检测效果，将本文模型 XGBoost-LightGBM 与 Wide & Deep CNN、WGAN、单个 XGBoost 和单个 LightGBM 模型进行对比，选取 AUC 作为主要评判标准，实验结果如图 5 所示。

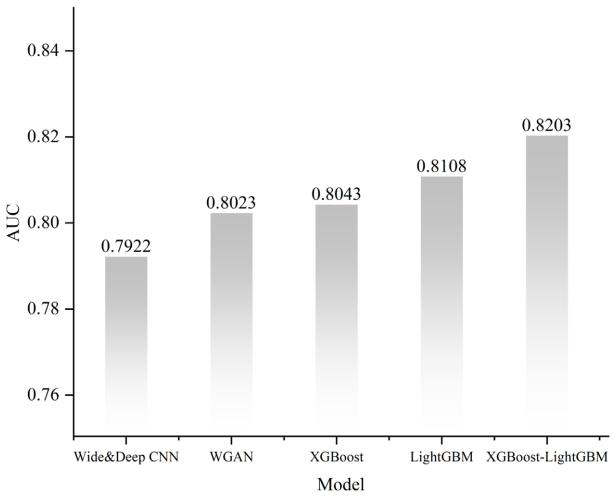


Figure 5. AUC performance comparison of model
图 5. 模型 AUC 性能对比

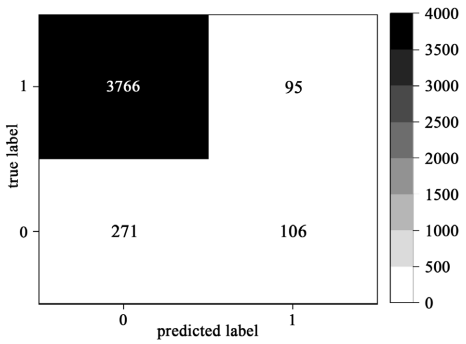
结果发现，本文模型 XGBoost-LightGBM 的 AUC 值较 Wide & Deep CNN、WGAN、单个 XGBoost 和单个 LightGBM 分别提升了 2.81%、1.8%、1.6%、0.95%。由此验证，基于树的 XGBoost 模型与 LightGBM 模型在电力表格数据异常检测方面具有一定的优势。

从而，本文将模型重点放在单个 XGBoost、单个 LightGBM 模型与 XGBoost-LightGBM 的融合模型的比较上，选取 Accuracy 和 G-mean 作为补充指标来验证集成模型与单个模型之间的效果，并绘制混淆矩阵进一步判断模型的可靠性。各模型的混淆矩阵如图 6 所示。

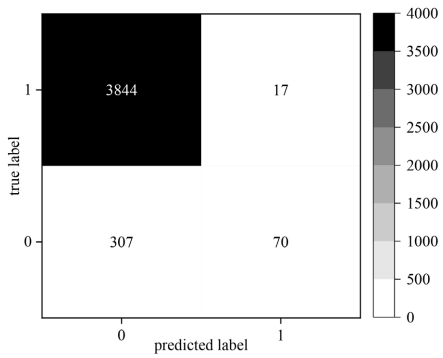
Table 2. Complete set of model metrics
表 2. 模型全部指标

模型	AUC	Accuracy	G-mean
XGBoost	0.8043	0.9136	0.5237
LightGBM	0.8108	0.9235	0.4300
XGBoost-LightGBM	0.8203	0.9153	0.5499

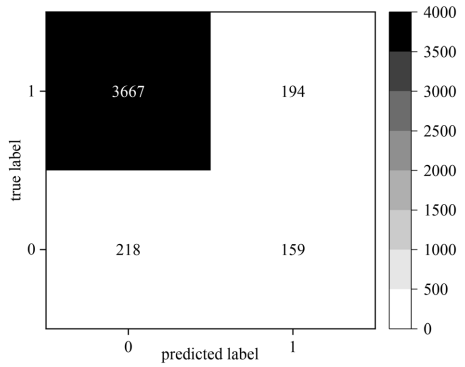
图 6 展示了单个 XGBoost、单个 LightGBM 模型与 XGBoost-LightGBM 融合模型的混淆矩阵，结合表 2 进行分析，可以看出尽管 XGBoost 模型的 AUC 为 0.8043，准确率达到 0.9136，但 TP 个数为 106，FP 个数为 95，其检出率仅为 0.2812，误检率为 0.0246。相较之下，LightGBM 模型表现略优，AUC 为 0.8108，准确率提升至 0.9235，然而 TP 个数为 70，FP 个数为 17，其检出率仍较低，仅为 0.1856，误检率为 0.0044。而融合模型在综合能力指标 AUC 上达到 0.8203，G-mean 指标达到了 0.5499，相较于 XGBoost 和 LightGBM 分别显著提升了 2.62%和 11.99%，同时 TP 个数为 159，FP 个数为 194，检出率高达 0.4215，相较于 XGBoost 和 LightGBM 分别提升了 23.58%和 14.04%。这一结果表明，该模型在整体性能上具有显著优势，尤其在识别少数类样本的能力上。



(a)



(b)



(c)

Figure 6. (a). XGBoost confusion matrix; (b). LightGBM confusion matrix; (c). XGBoost-LightGBM hybrid model confusion matrix
图 6. (a). XGBoost 混淆矩阵；(b). LightGBM 混淆矩阵；(c). XGBoost-LightGBM 融合模型混淆矩阵

4. 消融实验

为验证所提出的 XGBoost 与 LightGBM 动态权重融合机制的有效性，本文设计了消融实验，以此对比固定权重融合和动态权重融合的性能差异，将动态融合方法与以下几种基准方法进行对比，实验结果如图 7 所示。

a). fixed 0.5/0.5：固定等权融合

b). XGB only：仅用 XGBoost 模型

c). LGB only：仅用 LightGBM 模型

d). dynamic：动态权重融合

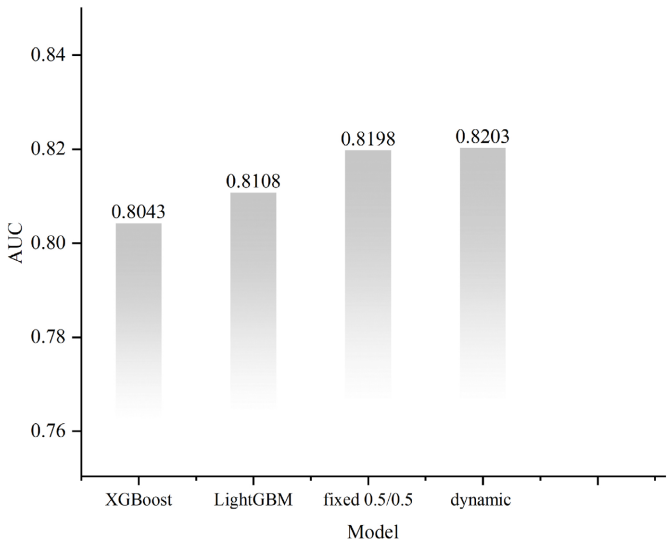


Figure 7. Performance comparison of ablation experiments
图 7. 消融实验性能对比

为进一步分析动态加权中平衡系数 α 对融合效果的影响，我们在 $\alpha \in [0, 1]$区间上以 0.1 为间隔逐步调整，并记录对应的 AUC 结果，结果如图 8 所示。

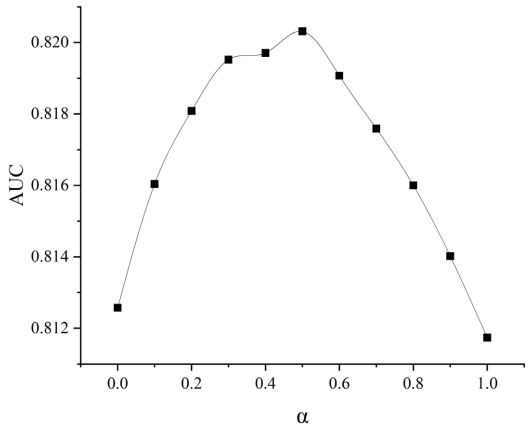


Figure 8. Performance comparison under different balancing coefficients α
图 8. 不同平衡系数 α 下的性能对比

结果表明，动态融合策略在 $\alpha=0.5$ 时取得最佳 AUC，相比固定等权和单模型均有提升，验证了该权重设计在保持模型性能稳定性的同时，能有效利用模型间的预测差异以增强泛化能力。此外，从 α 的调节曲线可观察到，当 α 较小时，权重更偏向 AUC 性能导向，模型融合更稳健；当 α 增大，差异性主导融合过程，增强了对异常样本的敏感性。因此，合理调节 α 可在性能稳定性与敏感性之间取得平衡。

5. 泛化性能对比实验

本节使用权威机器学习数据库 KEEL 中的 4 个不平衡数据集进行泛化性对比实验。在选择数据集时，保证数据集各类别样本数量、特征数量、不平衡率等特征有较大分布范围，从而增强实验结果的代表性与说服力，确保所得结论具有一定的通用性。各数据集的特征总结如表 3。

Table 3. Main features of the public dataset
表 3. 公开数据集主要特征

数据集	样本数量	特征数量	少数类样本数	多数类样本数	不平衡率
tic-tac-toe	958	9	332	626	1.89
pima	768	8	268	500	1.87
spambase	4597	57	1812	2785	1.54
wdbc	569	30	212	357	1.68

Table 4. Performance on the public dataset
表 4. 公开数据集性能

数据集	AUC	Accuracy	G-mean
tic-tac-toe	0.9131	0.8526	0.7303
pima	0.8792	0.8182	0.7781
spambase	0.9750	0.9457	0.9412
wdbc	0.9985	0.9649	0.9579

将上述数据集放入本文模型进行实验，结果见表 4 发现，本文模型在多个不同数据集上均表现出显著优势。其中，针对不平衡率最高的 tic-tac-toe 数据集，模型的 G-mean 值达到了 0.7303，AUC 值达到了 0.9131，Accuracy 值达到 0.8526，这表明模型对少数类样本学习的充足有效性；而对于样本数量较多且不平衡率低的 spambase 数据集，AUC、G-mean 和 Accuracy 值都提升至了 0.9750、0.9412、0.9457，这表

明对于不平衡样本来说，模型在不同不平衡率和不同特征维度的数据集上均保持稳定的性能，体现了该模型较强的泛化能力与鲁棒性。

6. 结论

为了解决窃电检测以及数据传输过程隐私保护的挑战，本研究在传统异常检测框架上进行了优化。其中，本文在传统异常检测框架上添加了数据传输过程中基于 RSA + AES 的混合加密隐私保护，并结合 SHA-256 加密哈希算法和数字签名技术；在异常检测模型训练环节，构建 XGBoost 与 LightGBM 的双模型融合式，使其对参数优化后的 XGBoost 与 LightGBM 模型实现以 AUC 与预测差异性为动态权重调整因子的自适应加权融合。

通过在国家电网公开数据集上的实验结果表明，本研究的融合模型在 AUC、和 G-mean 等关键指标上显著优于深度学习模型及传统单一的机器学习模型，该模型 AUC 值达 82.03%，准确率为 91.53%，G-mean 值为 54.99%。最后，将本文模型用于 4 个 KEEL 数据集上进行泛化性能测试，结果表明该模型具有显著的优势，在不平衡数据集上可以较好地检测出少数样本，提升异常检测的能力，并且也为电力盗窃防范提供了可靠的技术支持，展现出良好的应用潜力。

未来可进一步针对电表数据的时空关联特性进行针对性研究，以进一步提升窃电检测的精度。

基金项目

上海市哲学社会科学规划资助项目(2024BGL001)。

参考文献

[1] Glauner, P., Meira, J.A., Valtchev, P., State, R. and Bettinger, F. (2017) The Challenge of Non-Technical Loss Detection Using Artificial Intelligence: A Survey. *International Journal of Computational Intelligence Systems*, **10**, 760-775. https://doi.org/10.2991/ijcis.2017.10.1.51

[2] Jartelius, M. (2020) The 2020 Data Breach Investigations Report—A Cso's Perspective. *Network Security*, **2020**, 9-12. https://doi.org/10.1016/s1353-4858(20)30079-9

[3] Wang, X., Xie, H., Tang, L., Chen, C. and Bie, Z. (2024) Decentralized Privacy-Preserving Electricity Theft Detection for Distribution System Operators. *IEEE Transactions on Smart Grid*, **15**, 2179-2190. https://doi.org/10.1109/tsg.2023.3313771

[4] 周李, 赵露君, 高卫国. 稀疏编码模型在电力用户异常用电行为探测中的应用研究(英文) [J]. 电网技术, 2015, 39(11): 3182-3188.

[5] 许刚, 谈元鹏, 戴腾辉. 稀疏随机森林下的用电侧异常行为模式检测[J]. 电网技术, 2017, 41(6): 1964-1973.

[6] Xia, X., Xiao, Y. and Liang, W. (2019) ABSI: An Adaptive Binary Splitting Algorithm for Malicious Meter Inspection in Smart Grid. *IEEE Transactions on Information Forensics and Security*, **14**, 445-458. https://doi.org/10.1109/tifs.2018.2854703

[7] Zheng, Z., Yang, Y., Niu, X., Dai, H. and Zhou, Y. (2018) Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids. *IEEE Transactions on Industrial Informatics*, **14**, 1606-1615. https://doi.org/10.1109/tii.2017.2785963

[8] Nabil, M., Ismail, M., Mahmoud, M., Shahin, M., Qaraqe, K. and Serpedin, E. (2018) Deep Recurrent Electricity Theft Detection in AMI Networks with Random Tuning of Hyper-Parameters. 2018 24*th International Conference on Pattern Recognition* (*ICPR*), Beijing, 20-24 August 2018, 740-745. https://doi.org/10.1109/icpr.2018.8545748

[9] 张宇帆, 艾芊, 李昭昱, 等. 基于特征提取的面向边缘数据中心的窃电监测[J]. 电力系统自动化, 2020, 44(9): 128-134.

[10] Javaid, N., Jan, N. and Javed, M.U. (2021) An Adaptive Synthesis to Handle Imbalanced Big Data with Deep Siamese Network for Electricity Theft Detection in Smart Grids. *Journal of Parallel and Distributed Computing*, **153**, 44-52. https://doi.org/10.1016/j.jpdc.2021.03.002

[11] 高欣, 纪维佳, 赵兵, 等. 不平衡数据集下基于 CVAE-CNN 模型的智能电表故障多分类方法[J]. 电网技术, 2021, 45(8): 3052-3060.

[12] 严莉, 张凯, 徐浩, 等. 基于图注意力机制和 Transformer 的异常检测[J]. 电子学报, 2022, 50(4): 900-908.

[13] 蔡梓文, 赵云, 陆煜锌, 等. 基于变分自编码器的多源数据融合窃电检测方法[J]. 电力系统保护与控制, 2025, 53(4): 176-187.

[14] 游文霞, 申坤, 杨楠, 等. 基于 Bagging 异质集成学习的窃电检测[J]. 电力系统自动化, 2021, 45(2): 105-113.

[15] 李国成, 陆俊, 王赟, 等. 基于 Bagging 二次加权集成的孤立森林窃电检测算法[J]. 电力系统自动化, 2022, 46(2): 92-100.

[16] Naim, K., Khelifa, B. and Fateh, B. (2020) A Cryptographic-Based Approach for Electricity Theft Detection in Smart Grid. *Computers*, *Materials & Continua*, **62**, 97-117. https://doi.org/10.32604/cmc.2020.09391

[17] 史佳琪, 张建华. 基于多模型融合 Stacking 集成学习方式的负荷预测方法[J]. 中国电机工程学报, 2019, 39(14): 4032-4042.

[18] Shwartz-Ziv, R. and Armon, A. (2022) Tabular Data: Deep Learning Is Not All You Need. *Information Fusion*, **81**, 84-90. https://doi.org/10.1016/j.inffus.2021.11.011